QKD initiated by Authentication of EPR in 3 way channel

Abdulbast Abushgra, Khaled Elleithy
Computer Science & Engineering Department
University of Bridgeport, Bridgeport, CT

Abstract

Quantum key distribution (QKD) is one of the recent revolutions in cryptography field that was announced in first by Charles Bennett and Gilles Brassard in 1984. Here we create another QKD protocol that based on the three channel to communicate between two parties, and also ensures the connection is never established without providing the right identity in the first channel. Therefore, using the EPR pair in the first channel to approve the authentication in short time.

Introduction

The proposed protocol employs different approaches to fulfill the transformations between Alice (the sender) and Bob (the receiver) to prevent any leaking of data by Eve (eavesdropper). The protocol establishes with creating n EPR pair by Alice to affirm the authentication, if this was approved. Then Alice starts another type of quantum communication that based on two quantum bases in four states. Before submitting the photons Alice creates the matrix of random numbers that should be made as in the figure (). Next Alice sends the sequence of the Qubits to Bob, he should knows the time of starting the connection and also the length of submitted photons.

1								
2	1							
3	0	1						
4	1	1	0					
5	0	1	0	1				
6	0	0	1	0	1			
7	1	0	1	0	0	1		
8	1	1	0	1	1	0	0	

Parity cell
Index
Code Row

Figure (1) shows the preparation of the Qubits before sending to Bob.

4	1	1	0		x	x	x	x
6	0	0	1	0	1		x	x
2	1		x	x	x	x	x	x
8	1	1	0	1	1	0	0	
1		x	x	x	x	x	x	x
3	0	1		x	x	x	x	x
7	1	0	1	0	0	1		x
5	0	1	0	1		x	x	x

Parity cell
Index
Code Row

Figure (2) shows the preparation of the Qubits ready to be submitted to Bob.

The scheme diagram

Three channels will be initiated in this protocol, which begins with EPR pair, Four States channel, and then the classical channel that will be reduced in this protocol to just confirmation between the two parties of the communication.

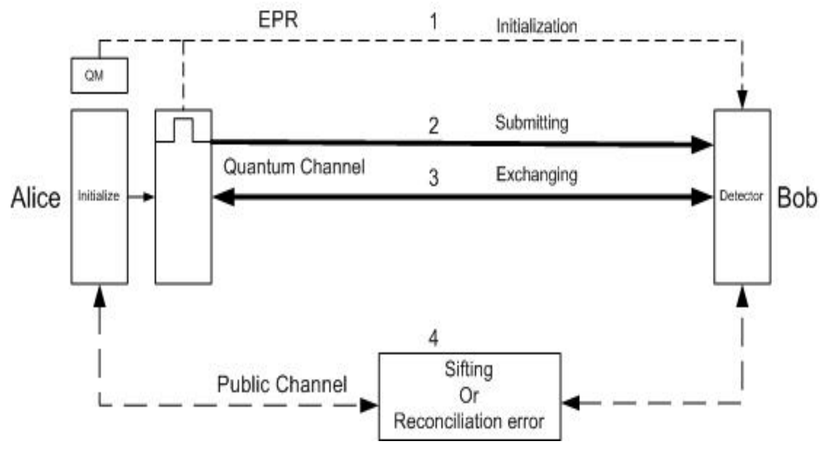

Figure (3) shows the new scheme of QKD.

Form of Transmission

Alice here sends the string of photons in the four states as fallows:

$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Bob on the side will measure the Qubits in one of the random Pauli-Matrices

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$
$$\sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Simulations

These simulations were made in different number of photons on both the new scheme and the BB84, where the noise channel was the same on both protocols.

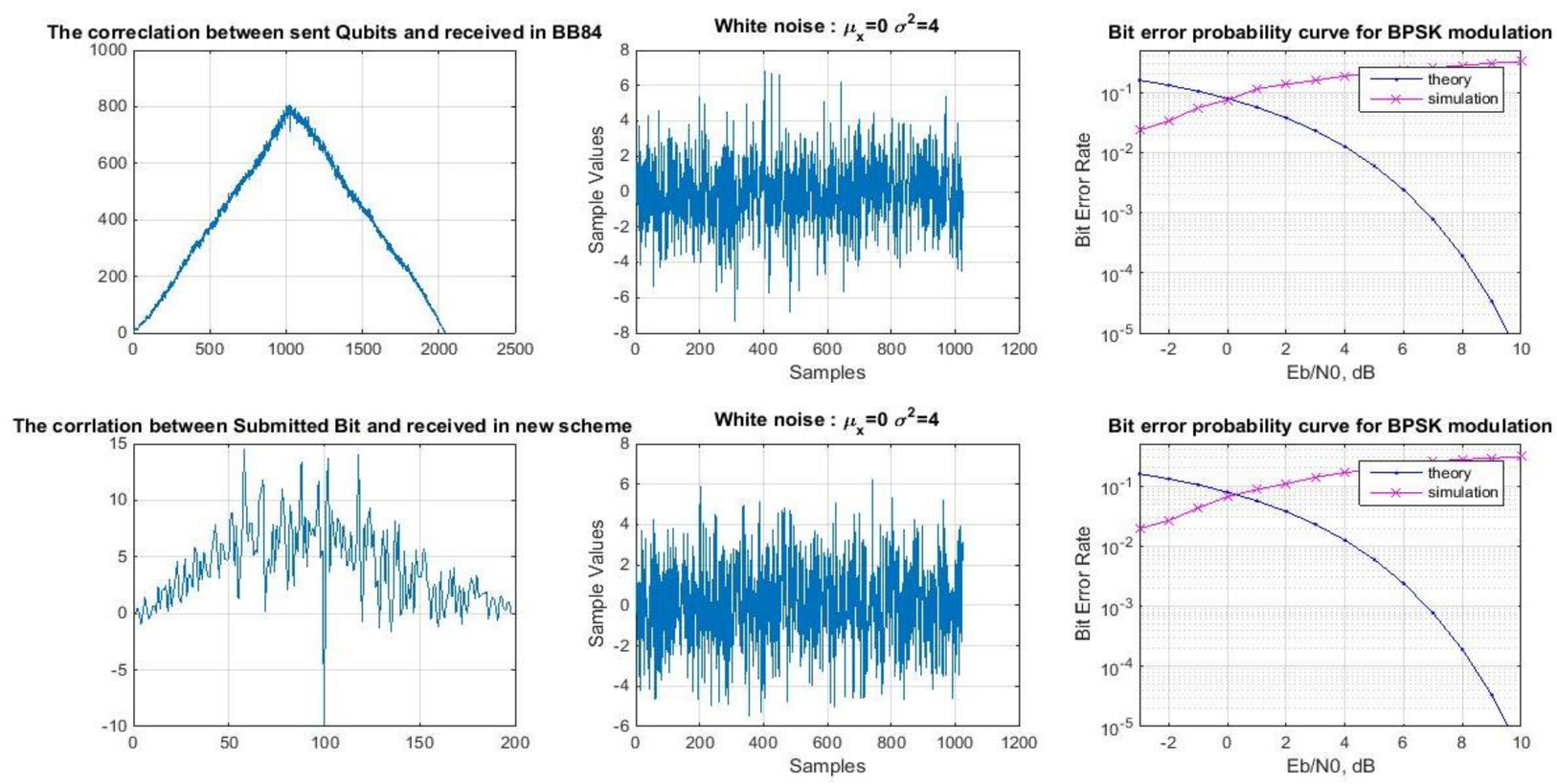

Figure (4) shows the simulation between the new scheme and the BB84.

Conclusion

- Our protocol has proved more security against the noisy that will be created by the eavesdropper or communications means (Fiber optic, or free space).
- Using the decoy state reduces the amount of losing photons.
- Correcting the errors into the communication channel supports the protocol to make early decision before going to classical channel.
- Some studies are still on this protocol to improve how to be used without quantum computers (our system now).

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, p. 441, 2000.
[3] A. A. Valerio Scarani, Gregoire Ribordy and Nicolas Gisin, "Quantum cryptography protocols robust against photon number splitting attacks," p. 2, 2004.
[4] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, p. 057901, 2004.
[5] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, p. 777, 1935.

Posted in Faculty Day Research @ 2015